1.    In a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from sending domains, a method for determining a sending domain's electronic message transmission policies, the method comprising:

an act of receiving an electronic message from the sending domain;

an act of receiving one or more electronic message transmission policies corresponding to the sending domain;

an act of parsing relevant electronic message transmission policies from the one or more received electronic message transmission policies; and

an act of providing the relevant electronic message transmission policies to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

2.    The method as recited in claim 1, wherein the act of receiving an electronic message from the sending domain comprises an act of receiving an electronic mail message.

3.    The method as recited in claim 1, wherein the act of receiving one or more electronic message transmission policies corresponding to the sending domain comprises an act of receiving one or more electronic message transmission policies included in the received electronic message.

4.    The method as recited in claim 3, wherein the act of receiving one or more electronic message transmission policies included in the received electronic message

Docket No. 13768.418.2

comprises an act of receiving one or more electronic message transmission policy certificates.

5. The method as recited in claim 4, wherein the act of receiving one or more electronic message transmission policies comprises an act of receiving proof-of-freshness for at least one of the one or more electronic message transmission policies.

6. The method as recited in claim 3, wherein the act of receiving one or more electronic message transmission policies included in the received electronic message comprises an act of receiving an ETP S/MIME message.

7. The method as recited in claim 6, wherein the act of receiving an ETP S/MIME message comprises an act of receiving a proof-of-freshness indication for a certificate

8. The method as recited in claim 1, further comprising:

an act of querying a server for electronic message policies corresponding to the sending domain.

9. The method as recited in claim 8, wherein the act of querying a name server for electronic message policies corresponding to the sending domain comprises an act of querying a DNS server.

10. The method as recited in claim 1, wherein the act of receiving one or more electronic message transmission policies corresponding to the sending domain comprises an act of receiving one or more electronic message transmission policy certificates from a server.

11. The method as recited in claim 10, wherein the act of receiving one or more electronic message transmission policy certificates from a server comprises an act of receiving at least electronic policy message certificate wherein the at least one electronic policy message certificate is an X.509 certificate, an XrML license, or a Kerberos PAC.

12. The method as recited in claim 1, wherein the act of receiving one or more electronic message transmission policies corresponding to the sending domain comprises an act of receiving one or more DNS TXT records.

13. The method as recited in claim 12, wherein the act of receiving one or more DNS TXT records comprises an act of receiving at least one DNS TXT record that resides in a sub-domain of the sending domain

14. The method as recited in claim 10, wherein the act of receiving one or more electronic message transmission policies corresponding to the sending domain comprises an act of receiving one or more DNS TXT records that encode the electronic message transmission policies in XML instructions.

15.    The method as recited in claim 14, wherein an act of receiving one or more DNS TXT records that encode the electronic message transmission policies in XML instructions comprises an act of receiving information that spans across a plurality DNS TXT records such that the electronic message configuration information can be concatenated into an XML instance.

16.    The method as recited in claim 15, wherein the act of receiving information that spans across a plurality DNS TXT records such that the electronic message configuration information can be concatenated into an XML instance comprises an act of receiving a plurality of DNS TXT records that include ordering data indicating how the XML instructions contained in the DNS TXT records are to be ordered.

17.    The method as recited in claim 16, further comprising:

an act of concatenating the XML instructions according to the ordering data to generate an XML instance.

18.    The method as recited in claim 1, wherein the act of parsing relevant electronic message transmission policies from the one or more received electronic message transmission policies comprises an act of parsing one or more electronic message policy certificates for relevant electronic message transmission policies.

19.     In a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from sending domains, a method for determining a sending domain's electronic message transmission policies, the method comprising:

an act of receiving an electronic message from the sending domain;

a step for identifying relevant electronic message transmission policies adhered to by the sending domain; and

an act of providing the relevant electronic message transmission policies to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

20.     The method as recited in claim 19, wherein the step of identifying electronic message transmission policies adhered to by a domain comprises an act of determining that the sending domain does not adhere to any electronic message transmission policies.

Docket No. 13768.418.2

21. In a sending domain that is network connectable to one or more receiving domains, the sending domain including a sending messaging server configured to send electronic messages to the receiving domains, a method for indicating to a receiving side domain that the sending messaging server expended computational resources to solve a computational puzzle before sending an electronic message to the receiving side domain, the method comprising:

an act of receiving electronic message data that is to be contained in an electronic message;

an act of generating an initial document from different portions state information;

an act of generating puzzle input from one or more components of the electronic message, the one or more components selected from among at least a message body, a message attachment, and a message header, puzzle input generation including one or more of extracting portions of a component, hashing portions of a component, and concatenating portions of a component;

an act of identifying an answer document such that an answer hash value, calculated from a combination of the answer document and the puzzle input hash value, is an answer value for a computational puzzle, the answer value being calculated using a puzzle hash algorithm; and

an act of sending an electronic message that includes the identified answer document and the electronic message data to the receiving side domain.

22.     The method as recited in claim 21, wherein the act of receiving electronic message data that is to be contained in an electronic message comprises an act of receiving electronic message data that is to be contained in an electronic mail message.

23.     The method as recited in claim 21, wherein the act of generating an initial document from different portions of state information comprises an act of extracting data from at least one field of the electronic message data wherein the at least one field is selected from a From field, a To field, a NotBefore field, a NotAfter field, a Date field, a Body field, an Attachment field, a Subject field, and a Message-Id field.

24.     The method as recited in claim 21, wherein the act of generating an initial document from different portions of state information comprises an act of extracting data from one or more date range fields.

25.     The method as recited in claim 21, wherein the act of generating an initial document from different portions of the state information comprises an act of extracting data wherein the data is text data, graphical data, Uniform Resource Identifier ("URI") data, or executable data.

26.     The method as recited in claim 21, wherein the act of identifying an answer document comprises an act of identifying an answer document that, when combined with the puzzle input and the combination of the answer document and puzzle input is hashed, results in a hash value having a specified value in a plurality of fixed bit positions.

27.     The method as recited in claim 26, wherein the act of identifying an answer document comprises an act of identifying an answer document that, when preprended to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having a value of zero in at least a first specified number of bits..

28.     The method as recited in claim 21, wherein the act of identifying an answer document comprises an act of identifying an answer document that, when concatenated to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having specified bit values in a first plurality of bit positions and having bit values equal to the corresponding bit values of in the hashes resulting from other answer documents in a second plurality of bit positions.

29.     The method as recited in claim 28, wherein the act of identifying an answer document comprises an act of identifying an answer document that, when concatenated to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having specified values in each bit position of a hash value prefix and a value equal to corresponding hash bit values resulting from other answer documents in a hash value suffix.

30.     The method as recited in claim 21, wherein the act of identifying an answer document comprises an act of using an puzzle hash algorithm, the puzzle hash algorithm being specifically designed to increase the difficulty of implementing hardware acceleration of the puzzle hash algorithm.

Docket No. 13768.418.2

31.    The method as recited in claim 21, wherein the act of identifying an answer document comprises an act of calculating an answer hash value using a hashing algorithm that alters the standard application of SHA-1 sub-functions.

32.    The method as recited in claim 21, wherein the act of sending an electronic message that includes the identified answer document and the electronic message data to the receiving side domain comprises an act of sending an electronic message that includes a plurality of answer documents.

33.    The method as recited in claim 21, further comprising:

an act of querying a server to determine if the receiving domain is configured to verify answers to computational puzzles; and

an act of receiving one or more DNS TXT records that contain electronic message configuration information for the receiving domain.

34.    The method as recited in claim 32, wherein the act of querying a server comprises an act of querying a server in response to the sending domain not supporting electronic mail transmission policy certificates.

35.    The method as recited in claim 32, wherein the act of receiving one or more DNS TXT records comprises an act of receiving one or more DNS TXT records that encode the electronic message configuration information in XML instructions

Docket No. 13768.418.2

36. In a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from the sending domains, a method for determining if a sending messaging server solved a computational puzzle before sending an electronic message, the method comprising:

an act of receiving an electronic message that includes electronic message data and an answer document;

an act of reproducing an initial document from different portions state information contained in the message;

an act of recalculating a puzzle input from one or more components of the electronic message, the one or more components selected from among at least a message body, a message attachment, and a message header, puzzle input generation including one or more of extracting portions of a component, hashing portions of a component, and concatenating portions of a component;

an act of determining if a verifying hash value, calculated from a combination of an answer document and the puzzle input hash value, is an answer value indicative of a solution to the computational puzzle, the verifying hash value being calculated using a puzzle hashing algorithm; and

an act of providing results of the determination to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

37.     The method as recited in claim 36, wherein the act of receiving an electronic message that includes electronic message data and an answer document comprises an act of receiving an electronic mail message.

38.     The method as recited in claim 36, wherein the act of receiving an electronic message that includes electronic message data and an answer document comprises an act of receiving an electronic message that includes a plurality of answer documents.

39.     The method as recited in claim 36, wherein the act of reproducing an initial document from different portions of state information contained in the electronic message comprises an act of extracting data from a field of the electronic message data wherein the field is selected from among a From field, a To field, a NotBefore field, a NotAfter field, a Date field, a Body field, an Attachment field, a Subject field, and a Message-ID field.

40.     The method as recited in claim 36, wherein the act of reproducing an initial document from different portions of state information contained in the electronic message comprises an act of extracting data from the electronic message data wherein the data is text data, graphical data, Uniform Resource Identifier ("URI") data, or executable data.

41.     The method as recited in claim 36, wherein the act of recalculating a puzzle input from one or more components of the electronic message comprises an act of applying an altered hashing algorithm, the altered hashing algorithm being specifically designed to increase the difficulty of implementing hardware acceleration that can be used to enhance efficiency of altered hashing algorithm.

42.    The method as recited in claim 36, wherein the act of recalculating a puzzle input from one or more components of the electronic message comprises an act of applying a hashing algorithm that alters the standard application of SHA-1 sub-functions.

43.    The method as recited in claim 36, wherein the act of determining if a verifying hash value, calculated from a combination of an answer document and the puzzle input, is an answer value indicative of a solution to the computational puzzle comprises an act of determining if the verifying hash value has a specified value in a plurality of fixed bit positions interspersed throughout the verifying hash value.

44.    The method as recited in claim 36, wherein the act of determining if a verifying hash value, calculated from a combination of an answer document and the puzzle input, is an answer value indicative of a solution to the computational puzzle comprises an act of determining if the verifying hash value has a specified value in a first plurality of bit positions and has a value equal to other verifying hash values resulting from other answer documents in a second plurality of bit positions.

45.     A computer program product for use in a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from sending domains, the computer program product for implementing a method for determining a sending domain's electronic message transmission policies, the computer program product comprising one or more computer-readable media having stored thereon computer executable instructions that, when executed by a processor, cause the receiving domain to perform the following:

receive an electronic message from the sending domain;

receive one or more electronic message transmission policies corresponding to the sending domain;

parse relevant electronic message transmission policies from the one or more received electronic message transmission policies; and

provide the relevant electronic message transmission policies to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

Docket No. 13768.418.2

46.    A computer program product for use in a sending domain that is network connectable to one or more receiving domains, the sending domain including a sending messaging server configured to send electronic messages to the receiving domains, the computer program product for implementing a method for indicating to a receiving side domain that the sending messaging server expended computational resources to solve a computational puzzle before sending an electronic message to the receiving side domain, the computer program product comprising one or more computer-readable media having stored thereon computer executable instructions that, when executed by a processor, cause the sending domain to perform the following:

receive electronic message data that is to be contained in an electronic message;

generate an initial document from different portions state information;

generate puzzle input from one or more components of the electronic message, the one or more components selected from among at least a message body, a message attachment, and a message header, puzzle input generation including one or more of extracting portions of a component, hashing portions of a component, and concatenating portions of a component;

identify an answer document such that an answer hash value, calculated from a combination of the answer document and the puzzle input hash value, is an answer value for a computational puzzle, the answer value being calculated using a puzzle hash algorithm; and

send an electronic message that includes the identified answer document and the electronic message data to the receiving side domain.

47.    A computer program product for use in a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from the sending domains, the computer program product for implementing a method for determining if a sending messaging server solved a computational puzzle before sending an electronic message, the computer program product comprising one or more computer-readable media having stored thereon computer executable instructions that, when executed by a processor, cause the receiving domain to perform the following:

receive an electronic message that includes electronic message data and an answer document;

reproduce an initial document from different portions state information contained in the message;

recalculate a puzzle input from one or more components of the electronic message, the one or more components selected from among at least a message body, a message attachment, and a message header, puzzle input generation including one or more of extracting portions of a component, hashing portions of a component, and concatenating portions of a component;

determine if a verifying hash value, calculated from a combination of an answer document and the puzzle input hash value, is an answer value indicative of a solution to the computational puzzle, the verifying hash value being calculated using a puzzle hashing algorithm; and

provide results of the determination to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

48.     A computer program product for use in a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from the sending domains, the computer program product for implementing a method for generating inputs to be provided to a message classification module, the computer program product comprising one or more computer-readable media having stored thereon computer executable instructions that, when executed by a processor, cause the receiving domain to perform the following:

receive an electronic message;

utilize one or more of a plurality of different mechanisms for attempting to determine if the received electronic message is an unwanted or an unsolicited electronic message; and

provide results of each of the one or more different mechanisms to a message classification module such that the message classification module can make a more reliable decision when classifying the received electronic message.

49.     The computer program product as recited in claim 48, wherein computer-executable instructions that, when executed, cause the receiving domain to utilize one or more of a plurality of different mechanisms for attempting to determine if the received electronic message is an unwanted or an unsolicited electronic message, comprise computer-executable instructions that, when executed, cause the receiving domain to utilize one or more of checking for adherence to an electronic mail transmission policy and checking for proof of effort by a sending domain.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Docket No. 13768.418.2